Charles Darwin School
Online Safety Policy

Persons Responsible:

Governors:	Full Governing Body
SLT:	Mrs L Rees
Written by:	Mr J Simpson, Online Safety Co-ordinator

Formally adopted by the Ethos Committee:	2 February 2015
Reviewed and readopted:	29 June 2015
Reviewed and readopted:	7 June 2021
Reviewed and readopted:	1 October 2024

Table of Contents

1. Who will write and review the policy?

1.1. The Online Safety Policy will be reviewed annually by Mr Simpson (Online Safety Co-ordinator) and Naj Naseer (Network Manager). This Online Safety Policy has been written by the school, building on the KCC Online Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by governors. When staff and pupils leave the school their account or rights to specific school areas will be disabled by the IT Technical Department. At the start of the school year students in Year 7 are requested to sign AUP as part of the home school agreement outlines the rules and regulations in regards to computer use in the school. The school has an appointed Online Safety Co-ordinator, Mr Simpson who will work closely with the Designated Child Protection Officer.

1.2. This policy should be read in conjunction with the school's Safeguarding Policy [which includes PREVENT awareness], the Anti-bullying Policy, attendance Policy and PSHE Policy.

2. Why is internet use important?

2.1. Internet use is part of the statutory curriculum and a necessary tool for learning. The internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.

3. How does internet use benefit education?

3.1. The internet allows access to experts in many fields for both pupils and staff. It allows collaboration across networks of schools, support services and professional associations. It also gives us access to learning wherever and whenever.

4. How can internet use enhance learning?

4.1. The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for internet use. Staff should guide pupils to online activities that will support the learning outcomes planned for pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

5. How will pupils learn how to evaluate Internet content?

5.1. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is part of teaching/learning in every subject.

6. How will information systems security be maintained?

6.1. Virus protection software (Sophos) will be updated regularly by the network manager. The security of the school information systems and users will also be reviewed regularly by the Network Manager and SLT. Unapproved software will not be allowed in pupils' work areas or attached to email. Files held on the school's network will be checked when necessary. The network manager will review system capacity regularly. The school internet access will be designed to enhance and extend education and this will be the job of the network manager and SLT. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

6.2. All staff have had PREVENT duty training regarding radicalisation and extremism and are aware of the necessary referral process if they feel the school's IT systems are being misused.

7. How will e-mail be managed?

7.1. Pupils must immediately tell a member of staff if they receive offensive email. This can then be passed on to the relevant people (Online Safety Coordinator, ACo, Network Manager) so that further sanctions can be taken where necessary. Pupils must not reveal their own or others' personal details in email communication or arrange to meet anyone without specific permission from an adult. It is the responsibility of the Online Safety Coordinator to make sure pupils understand this through assemblies, tutor programmes etc.

8. How will published content be managed?

8.1. The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. Email addresses should be published carefully to avoid being harvested for spam. Atomwide filter used to help this process. The Online Safety Coordinator together with the network manager will take overall responsibility and ensure that content is accurate and appropriate.

9. How will social networking, social media and personal publishing be managed?

9.1. The school will block/filter access to social networking sites and newsgroups will be blocked unless specific use is approved. This will be managed by the Network Manager. Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline numbers, schools attended, IM and e-mail addresses, full names of friends, specific interests and clubs. Work is done through tutor programmes, assemblies and taught in ICT lessons to Year 8. Pupils should be advised not to place personal photos on any social network sites. They should be taught to consider how public the information is and consider using private areas. Teachers should be advised not to run social network spaces for student use on a personal basis. This message should come from SLT. Pupils

should be advised through IT lessons on security issues surrounding ICT and be encouraged to set passwords, deny unknown individuals and block unwanted comments. Students should be encouraged not to publish specific and detailed private thoughts.

10. How will filtering be managed?

10.1. The Network Manager will be responsible for blocking unsuitable sites and if staff or pupils discover these then they should be reported to the Network Manager in the first instance. Atomwide will be used as basic filtering tool. The Network Manager will also be responsible for ensuring that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Pupils should be encouraged to report to appropriate agencies such as CEOP if they find any illegal material or content.

10.2. The network manager and IT staff are all PREVENT duty trained and are aware of the importance of blocking unsuitable sites around radicalisation and extremism.

11. How can emerging technologies be managed?

11.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones are not allowed in lessons or formal school time (see separate policy). The sending of abusive or inappropriate text messages is forbidden. No third party devices are allowed on-site as well as no phone use within school. Staff will be issued with a school phone where contact with pupils/parents is required.

12. How should personal data be protected?

12.1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR).

13. How will internet access be authorised?

13.1. All staff and pupils have access to the school's electronic communications. All staff must read and sign a "Guardian statement" when they collect their staff laptop which outlines acceptable use. Pupils sign an AUP at the start of Year 7 which outlines acceptable use including Internet use.

14. How will Online Safety complaints be handled?

14.1. Complaints of computer misuse will be reported to a member of staff, the Network Manager who will in turn inform the Online Safety Co-ordinator. The incident is then logged and appropriate sanction(s) given including a conversation with parents. Any complaint about staff misuse must be referred to the Head Teacher. Pupils and parents have access to the complaints procedure via the website. Parents and pupils will need to work in partnership with the school to resolve issues. All Online Safety complaints and incidents will be recorded by the school, including any actions taken.

15. How is the internet used across the community?

15.1. The school will be sensitive to internet related issues experienced by pupils out of school e.g. social networking sites and offer appropriate advice. There is a secure, unfiltered PC in the IT office to help facilitate this. This can also help with incidents of Cyberbullying (see below).

16. How will cyberbullying be managed?

16.1. Cyberbullying awareness is taught to all students as part of the curriculum in Year 8. It is also taught to students through a series of assemblies and as part of year groups' tutorial programmes (Year 7 – 11). Cyberbullying will not be tolerated in school. There will be clear procedures in place and all incidents of Cyberbullying reported to the school will be recorded.

16.2. This policy should be read in conjunction with the school's Safeguarding Policy and the Anti-bullying Policy.

17. How will learning platforms and learning environments be managed?

17.1. Pupils and staff will be advised on acceptable conduct and use when using the learning platform. Only members of the current pupil, parent/carers and staff community will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

18. How will the policy be introduced to pupils?

18.1. Online Safety rules will be posted in rooms with Internet access. Users will be informed that network and Internet use will be monitored. Safe and responsible use of the Internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

19. How will the policy be discussed with staff?

19.1. The Online Safety Policy will be available for all staff to view in the staffroom and website.

20. How will parents' support be enlisted?

20.1. A partnership approach with parents will be encouraged. Parents are invited to attend an annual Online Safety evening where they will be informed about the issues and dangers surrounding Online Safety and ways in which they can help identify the behaviours exhibited by individuals. Information and guidance will also be made available to parents and guardians during these evening and through the school website.